

ABSTRACT

Described is a system and method whereby processes may have multiple memory maps associated therewith to provide curtailed memory and overcome other memory-related problems.

5 Multiple maps are used to restrict memory access of existing code such as drivers, without changing that code, and without changing existing microprocessors. A thread of a process is associated with one memory map at a time, which by mapping to different memory locations, provides memory isolation without requiring a process switch. Memory isolation may be combined with controlled, closed memory map switching performed only by trusted code, to ensure that some protected memory is inaccessible to all but the trusted code (curtailed memory). For example, the threads of the process may ordinarily run at one privilege level with a restricted map, with map switching is only allowed at a higher privilege level. As the threads run through code, the map may be appropriately changed on entering and leaving the trusted code, thus controlling what memory addresses are accessible based on what code is

10

15

20 currently being executed. Map switching among multiple maps eliminates the need to change a process in order to access different memory, thereby allowing expanded memory addressing in a single process and isolating untrusted code run in process from certain memory of that process.